IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

IDENITY SECURITY LLC, Plaintiff, v. APPLE, INC. Defendant.	Civil Action No. 6:21-CV-460 Jury Trial Demanded

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT AND JURY DEMAND

Plaintiff Identity Security LLC ("Identity Security" or "Plaintiff") files this Original Complaint for Patent Infringement and Jury Demand against Defendant Apple, Inc. ("Apple" or "Defendant"), alleging as follows:

The Parties

1. Plaintiff Identity Security LLC is a Texas limited liability company having its principal place of business at 1310 Welch Street, Unit A, Houston, Texas 77006.

2. Identity Security is the owner of U.S. Patent No. 7,493,497, U.S. Patent No. 8,020,008, U.S. Patent No. 8,489,895, and U.S. Patent No. 9,507,948 (collectively, the "Patents-in-Suit").

3. Defendant Apple Inc. is a California corporation with a principal place of business at One Apple Park Way, Cupertino, California 95014. Apple can be served through its registered agent, CT Corporation System, 818 W. Seventh Street, Suite 930, Los Angeles, California, 90017.

4. Apple is registered to do business in Texas and has regular and established places of business in this District, including at 3121 Palm Way, Austin, Texas, 2901 S. Capital of Texas Hwy., Austin, Texas,12535 Riata Vista Circle, Austin, Texas, and 5501 West Parmer Lane, Austin, Texas. Apple employs thousands of people at these locations in Texas. Upon information and

belief, work done at these Apple locations in Texas includes work related to device security and Apple's Secure Enclave.

5. Apple has placed or contributed to placing infringing products, including iPhones, iPads, Apple Watches, and MacBook computers, into the stream of commerce via an established distribution channel knowing or understanding that such products would be sold and used in the United States, including in the Western District of Texas.

6. On information and belief, Apple also has derived substantial revenues from infringing acts in the Western District of Texas, including from the sale and use of infringing products, including iPhones, iPads, Apple Watches, and MacBook computers.

Jurisdiction and Venue

7. This is an action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

8. This Court has specific personal jurisdiction over Apple because Apple conducts business in the State of Texas and in this District. Plaintiff's causes of action arise from Apple's contacts with and activities in the State of Texas and in this District. Upon information and belief, Apple has committed acts of infringement within the State of Texas and within this District by directly and/or indirectly making, using, selling, offering to sell, or importing products that infringe one or more claims of the Patents-in-Suit.

9. Defendant has committed acts within this District giving rise to this action and has established sufficient minimum contacts with the State of Texas such that the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

10. Venue is proper in this District under 28 U.S.C. § 1391(b), (c), and 1400(d) because (1) Defendant has done and continues to do business in this District, (2) Defendant has a regular and established place of business in this District, and (3) Defendant has committed and continues to commit acts of patent infringement in this District by using, selling, offering to sell, or importing products that infringe one or more claims of the Patents-in-Suit. In particular, Apple maintains regular and established places of business in this District, including, at 3121 Palm Way, Austin, Texas, 2901 S. Capital of Texas Hwy., Austin, Texas, 12535 Riata Vista Circle, Austin, Texas, and 5501 West Parmer Lane, Austin, Texas. Apples carries out its business from these physical locations.

The Patents-in-Suit

11. Identity Security is the owner of U.S. Patent No. 7,493,497 ("the '497 Patent") titled "Digital Identity Device," a true and correct copy of which is attached as Exhibit 1. The U.S. Patent and Trademark Office duly issued the '497 Patent on February 17, 2009. The '497 Patent is valid and enforceable.

12. Identity Security is the owner of U.S. Patent No. 8,020,008 ("the '008 Patent"), titled "Microprocessor Identity Device," a true and correct copy of which is attached as Exhibit 2. The U.S. Patent and Trademark Office duly issued the '008 Patent on September 13, 2011. The '008 Patent is valid and enforceable.

13. Identity Security is the owner of U.S. Patent No. 8,489,895 ("the '895 Patent"), titled "Microprocessor Identity Device," a true and correct copy of which is attached as Exhibit 3. The U.S. Patent and Trademark Office duly issued the '895 Patent on July 16, 2013. The '895 Patent is valid and enforceable.

14. Identity Security is the owner of U.S. Patent No. 9,507,948 ("the '948 Patent"), titled "Digital Identity Device," a true and correct copy of which is attached as Exhibit 4. The U.S. Patent and Trademark Office duly issued the '948 Patent on November 29, 2016. The '948 Patent is valid and enforceable.

Background

15. The claims of the Patents-in-Suit disclose a novel and unconventional means of improving the privacy and security of digital information on a digital device using a unique microprocessor identity device, which is used to create a unique digital identity for the user. The combination of the unique microprocessor identity and digital identity for the user can be used to secure communications between parties and grant various levels of permission, as well as authenticate the identity of the users. *See, e.g.*, Exhibit 1 at 1:13-17.

16. Claim 1 of the '497 Patent is representative. Claim 1 states:

> 1. A digital identity device, comprising:
>
> a microprocessor comprising a microprocessor identity that uniquely identifies the microprocessor, wherein the microprocessor comprises an on-die Programmable Read-Only Memory (PROM) and the microprocessor identity is etched into the PROM;
>
> digital identity data, wherein the digital identity data identifies an owner of the digital identity device, wherein the digital identity data comprises a name of the owner;
>
> a memory configured to store at least the digital identity data, wherein the microprocessor identity is an alpha-numeric value, and
>
> wherein the digital identity data is bound to the microprocessor identity by encrypting the digital identity data using an algorithm that uses the microprocessor identity.

Under claim 1 of the '497 Patent, the microprocessor is uniquely identified using an alpha-numeric value that is etched, or programmed, into a programmable read-only memory or PROM. Further, the digital identity data corresponding to the user or owner is encrypted using an algorithm that uses the unique microprocessor identity. In other words, the unique microprocessor identity can be used as a cipher to protect the owner's identity and authenticate the user, thereby permitting authorized used of the device.

17. Claim 1 of the '008 Patent states:

> 1. A microprocessor identity device, comprising:
>
> a microprocessor;
>
> microprocessor identity information that uniquely identifies the microprocessor identity device
>
> digital identity data that identifies an owner of the microprocessor identity device; and
>
> and a memory operatively connected to the microprocessor and configured to store the digital identity data and the microprocessor identity information,
>
> wherein the digital identity data is bound to the microprocessor identity device by encoding, using the microprocessor, the digital identity data using an algorithm that uses the microprocessor identity information.

Claim 5 of the '895 states:

> 5. A microprocessor identity device, comprising:
>
> a microprocessor;
>
> microprocessor identity information that uniquely identifies the microprocessor identity device;
>
> and digital identity data that identifies an owner of the microprocessor identity device, the digital identity data being bound to the microprocessor identity device, wherein the digital identity data includes a password provided by the owner, and wherein the digital identity data is bound to the microprocessor identity device using an encryption algorithm and the microprocessor identity information.

Claim 1 of the '948 patent discloses a similar invention tied to biometric information. The claim states:

> 1. A digital identity device comprising:
>
> a microprocessor, wherein microprocessor identity information uniquely identifies the microprocessor;

> digital identity data that identifies an owner of the digital identity device,
>
> wherein the digital identity data is bound to the microprocessor by encrypting, using the microprocessor, the digital identity data using an algorithm that uses the microprocessor identity information,
>
> wherein the microprocessor reads the digital identity data,
>
> wherein the digital identity data comprises an owner's biometric information, and
>
> wherein the owner's biometric information comprises a fingerprint.

18. Uniquely identifying the microprocessor and then creating a unique digital identity wherein the digital identity is bound to the microprocessor using encryption, among other aspects of the invention, provides a novel approach to securing digital transactions. The microprocessor identity is unique to that device and distinguishes that device from others like it in the world. *See, e.g.*, Ex. 1 at 3: 63-65.

19. Apple infringes at least claim 1 of the ’497 Patent, claim 1 of the ’008 Patent, claim 5 of the ’895 Patent, and claim 1 of the ’948 Patent by making, using, selling, offering for sale, and/or importing into the United States products that incorporate Apple’s Secure Enclave. Attached as Exhibits 5-8 are claim charts showing infringement by Apple’s Secure Enclave processor of at least one claim from each of the Patents-in-Suit.

20. “The *Secure Enclave* is a system on chip (SoC) that is included on all recent iPhone, iPad, Apple Watch, Apple TV and HomePod devices, and on a Mac with Apple silicon as well as those with the Apple T2 Security Chip. … The Secure Enclave also provides the foundation for the secure generation and storage of the keys necessary for encrypting data at rest, and it protects and evaluates the biometric data for Touch ID and Face ID.” *See* https://support.apple.com/guide/security/hardware-security-overview-secf020d1074/1/web/1. Apple describes the Secure Enclave as “a hardware-based key manager that’s isolated from the main processor to provide an extra layer of security.” *See*

https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave. Apple described the benefits of using the Secure Enclave to developers: "When you store a private key in the Secure Enclave, you never actually handle the key, making it difficult for the key to become compromised. Instead, you instruct the Secure Enclave to create the key, securely store it, and perform operations with it. You receive only the output of these operations, such as encrypted data or a cryptographic signature verification outcome." *Id.*

21. The Secure Enclave was introduced as part of the Apple A7 processor in the iPhone 5S in September 2013. Since then, several Apple Products have used the Secure Enclave, namely:

- iPhone 5S and later
- iPad Air or later
- MacBook Pro computers with TouchBar that contain the Apple T1 Chip
- Intel-based Mac computers that contain the Apple T2 Security Chip
- Mac computers with Apple silicon
- Apple TV HD or later
- Apple Watch Series 1 or later
- HomePod and HomePod mini

("the Infringing Products"). https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web. Apple leverages the Secure Enclave in several applications and features. For example, the Secure Enclave plays a role in managing the authentication process and enabling payment transaction to proceed in Apple Pay. https://support.apple.com/guide/security/apple-pay-component-security-sec2561eb018/1/web/1. With Apple's Touch ID security:

> When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave. Communication between the processor and the Touch ID sensor takes place over a serial peripheral interface bus. The processor forwards the data to the Secure

> Enclave but can't read it. It's encrypted and authenticated with a session key that's negotiated using a shared key provisioned for each Touch ID sensor and its corresponding Secure Enclave at the factory.

https://support.apple.com/guide/security/touch-id-and-face-id-security-sec067eb0c9e/1/web/1.

22. Similarly, Face ID data is sent to the Secure Enclave. "A portion of the Secure Neural Engine—protected within the Secure Enclave—transforms this data into a mathematical representation and compares that representation to the enrolled facial data." *Id.*

23. Security of computers and mobile devices is paramount. As mobile devices and computers (including smart watches and tablets) have come to dominate our daily lives, the need to keep them secure becomes ever more critical. "Mobile security involves protecting portable devices such as laptops, tablets, smart watches, and phones against cyber threats. Today, the need for protection is more critical because we store a lot of sensitive data on these devices. Studies show that mobile banking is one of the top three most used apps by Americans. The case is similar in other countries especially in the developing and emerging markets. Most individuals and small businesses also use their smartphones and laptops to login into their emails and social media pages. With each day that passes, we are adding some data to our digital footprints through our mobile devices, making it easy for hackers to target us." *See* https://www.whatmobile.net/Opinion/article/mobile-security-important.

24. As another reporter put it, "Having a mobile phone has become a large part of our everyday life. Many underestimate the value a phone truly holds when it comes to the information it stores. Your phone has your entire life on it." https://blog.rsisecurity.com/importance-of-mobile-security/. This is not an exaggeration. In addition to email and social media accounts, mobile phones and computers contain sensitive personal and financial information as well as applications that permit users to access their bank accounts, credit card accounts, and mobile payment options. That data must be protected.

25. The claimed invention makes it more difficult for hackers to obtain sensitive information by, among other benefits, providing protection that is linked to the device's hardware, *e.g.,* the processor, which is given its own unique identifier. From there, the unique identifier can be used as a key against which other identifiers can be checked, encrypted, or otherwise protected.

Count One: Infringement of U.S. Patent No. 7,493,497

26. Plaintiff restates and incorporates by reference the allegations made in the preceding paragraphs as though fully set forth herein.

27. Apple has infringed, and is continuing to infringe, literally or under the doctrine of equivalents, at least claim 1 of the '497 Patent by making, using, selling, and/or offering for sale the Infringing Products in the United States, in violation of 35 U.S.C. § 271(a). Likewise, Defendant Apple has infringed, and is continuing to infringe, literally or under the doctrine of equivalents, at least claim 1 of the '497 Patent by importing the Infringing Products into the United States.

28. An example of Apple's infringement by the Secure Enclave is found in Exhibit 5 to this Complaint. By way of example, the digital identity devices, *i.e*., the Infringing Products, each comprise a microprocessor, the Secure Enclave, comprising a microprocessor identity that uniquely identifies the microprocessor, wherein the microprocessor comprises an on-die Programmable Read-Only Memory (PROM) and the microprocessor identity is etched into the PROM. The Secure Enclave is a coprocessor and is provisioned during fabrication with its own unique ID, which is an AES-256 bit key, *i.e*., an alpha-numeric value, fused to the coprocessor. The Infringing Products also each comprise digital identity data in the form of passcode, Touch ID, or Face ID data. Such data identify the owner of the device, including the name of the owner, which can be the name of an individual, the name of a company or organization, or other

identifying data. The digital identity data is stored in memory in or only available to the Secure Enclave and is bound to the Secure Enclave's unique ID by encrypting the data with a key entangled with the unique ID. The foregoing description is based on publicly available information and a reasonable investigation of the structure and operation of the Infringing Products. Plaintiff reserves the right to modify this description, including, for example, on the basis of information about the Infringing Products that it obtains during discovery.

29. Apple has had knowledge of the '497 Patent at least as of the date of this Complaint.

30. Apple's direct infringement has damaged and continues to damage Plaintiff in an amount yet to be determined, but at no less than a reasonable royalty.

Count Two: Infringement of U.S. Patent No. 8,020,008

31. Plaintiff restates and incorporates by reference the allegations made in the preceding paragraphs as though fully set forth herein.

32. Apple has infringed, and is continuing to infringe, literally or under the doctrine of equivalents, at least claims 1, 2, 4, 6, and 7 of the '008 Patent by making, using, selling, and/or offering for sale the Infringing Products in the United States, in violation of 35 U.S.C. § 271(a). Likewise, Defendant Apple has infringed, and is continuing to infringe, literally or under the doctrine of equivalents, at least claims 1, 2, 4, 6, and 7 of the '008 Patent by importing the Infringing Products into the United States.

33. An example of Apple's infringement by the Secure Enclave is found in Exhibit 6 to this Complaint. By way of example, the Infringing Products contain a microprocessor identity device, the Secure Enclave, that comprise a microprocessor wherein microprocessor identity information uniquely identifies the microprocessor identity device. The Secure Enclave is a coprocessor and is provisioned during fabrication with its own unique ID, which is an AES-256

bit key, *i.e.*, an alpha-numeric value. The Infringing Products also each comprise digital identity data in the form of passcode, Touch ID, or Face ID data that identify the owner of the device, including the name of the owner, which can be the name of an individual, the name of a company or organization, or other identifying data. The Secure Enclave also includes a memory operatively connected to the microprocessor that stores the digital identity data and the microprocessor identity information, wherein the digital identity data are bound to the microprocessor identity device by encoding, using the microprocessor, the digital identity data using an algorithm that uses the microprocessor identity information. The digital identity data are bound to the Secure Enclave's unique ID by encrypting the data with a key entangled with the unique ID. The foregoing description is based on publicly available information and a reasonable investigation of the structure and operation of the Infringing Products. Plaintiff reserves the right to modify this description, including, for example, on the basis of information about the Infringing Products that it obtains during discovery.

34. Apple has had knowledge of the '008 Patent at least as of the date of this Complaint.

35. Apple's direct infringement has damaged and continues to damage Plaintiff in an amount yet to be determined, but at no less than a reasonable royalty.

Count Three: Infringement of U.S. Patent No. 8,489,895

36. Plaintiff restates and incorporates by reference the allegations made in the preceding paragraphs as though fully set forth herein.

37. Apple has infringed, and is continuing to infringe, literally or under the doctrine of equivalents, at least claim 5 of the '895 Patent by making, using, selling, and/or offering for sale the Infringing Products in the United States, in violation of 35 U.S.C. § 271(a). Likewise, Defendant Apple has infringed, and is continuing to infringe, literally or under the doctrine of

equivalents, at least claim 1 of the ’895 Patent by importing the Infringing Products into the United States.

38. An example of Apple’s infringement by the Secure Enclave is found in Exhibit 7 to this Complaint. By way of example, the Infringing Products contain a microprocessor identity device, the Secure Enclave, that comprise a microprocessor wherein microprocessor identity information uniquely identifies the microprocessor identity device. The Secure Enclave is a coprocessor and is provisioned during fabrication with its own unique ID, which is an AES-256 bit key, *i.e.*, an alpha-numeric value. The Infringing Products also each comprise digital identity data in the form of passcode, Touch ID, or Face ID data that identify the owner of the device, including the name of the owner, which can be the name of an individual, the name of a company or organization, or other identifying data. The passcode, Touch ID, and Face ID can be viewed as passwords provided by the owner. The Secure Enclave also includes a memory operatively connected to the microprocessor that stores the digital identity data and the microprocessor identity information, wherein the digital identity data is bound to the microprocessor identity device by encoding, using the microprocessor, the digital identity data using an algorithm that uses the microprocessor identity information. The foregoing description is based on publicly available information and a reasonable investigation of the structure and operation of the Infringing Products. Plaintiff reserves the right to modify this description, including, for example, on the basis of information about the Infringing Products that it obtains during discovery.

39. Apple has had knowledge of the ’895 Patent at least as of the date of this Complaint.

40. Apple’s direct infringement has damaged and continues to damage Plaintiff in an amount yet to be determined, but at no less than a reasonable royalty.

Count Four: Infringement of U.S. Patent No. 9,507,948

41. Plaintiff restates and incorporates by reference the allegations made in the preceding paragraphs as though fully set forth herein.

42. Apple has infringed, and is continuing to infringe, literally or under the doctrine of equivalents, at least claim 1 of the '948 Patent by making, using, selling, and/or offering for sale the Infringing Products in the United States, in violation of 35 U.S.C. § 271(a). Likewise, Defendant Apple has infringed, and is continuing to infringe, literally or under the doctrine of equivalents, at least claim 1 of the '948 Patent by importing the Infringing Products into the United States.

43. An example of Apple's infringement by the Secure Enclave is found in Exhibit 8 to this Complaint. By way of example, the digital identity devices, *i.e.*, the Infringing Products, each comprise a microprocessor, the Secure Enclave, wherein microprocessor identity information uniquely identifies the microprocessor. The Secure Enclave is a coprocessor and is provisioned during fabrication with its own unique ID, which is an AES-256 bit key, *i.e.*, an alpha-numeric value. The Infringing Products also each comprise digital identity data in the form of Touch ID data that identify the owner of the device, including the name of the owner, which can be the name of an individual, the name of a company or organization, or other identifying data. The digital identity data is bound to the Secure Enclave's unique ID by encrypting the data with a key entangled with the unique ID. The Secure Enclave reads the digital identity data, which comprises biometric information, *i.e.*, fingerprint data. The foregoing description is based on publicly available information and a reasonable investigation of the structure and operation of the Infringing Products. Plaintiff reserves the right to modify this description, including, for example, on the basis of information about the Infringing Products that it obtains during discovery.

44. Apple has had knowledge of the ’948 Patent at least as of the date of this Complaint.

45. Apple’s direct infringement has damaged and continues to damage Plaintiff in an amount yet to be determined, but at no less than a reasonable royalty.

Jury Demand

46. Plaintiff demands a jury trial for all issues deemed to be triable by jury.

Prayer for Relief

Based on the foregoing, Plaintiff respectfully requests that this Court grant the relief set forth below:

a. A judgment that Defendant Apple has directly infringed, either literally or under the doctrine of equivalents, and continues to directly infringe, one or more claims of the ’497 Patent, the ’008 Patent, the ’895 Patent, and the ’948 Patent;

b. A judgment and order requiring Defendant Apple to pay Plaintiff damages under 35 U.S.C. § 284, and supplemental damages for any continuing post-verdict infringement through entry of the final judgment with an accounting as needed;

c. A judgment and order requiring Defendant Apple to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;

d. A judgment and order awarding a compulsory ongoing royalty;

e. A judgment granting a preliminary and permanent injunction that restrains and enjoins Defendant Apple, its officers, directors, employees, agents, servants, parents, subsidiaries, successors, assigns, and all those in privity, concert or participation with them from infringing the Patents-in-Suit.

f. Such other and further relief as the Court deems just and equitable.

Dated: May 3, 2021

Respectfully submitted,

SUSMAN GODFREY LLP

/s/ John P. Lahad
John P. Lahad
jlahad@susmangodfrey.com
Texas Bar No. 24068095
Brian D. Melton
bmelton@susmangodfrey.com
Texas Bar No. 24010620
Matt Wood
mwood@susmangodfrey.com
Texas Bar No. 24110548
1000 Louisiana Street, Suite 5100
Houston, Texas 77002
Tel: (713) 651-9366
Fax: (713) 654-6666

Attorneys for Plaintiff Identity Security LLC